	Application No.	Applicant(s)
Notice of Allowability	09/767,617	GOHL, ERIKA MONIKA
	Examiner	**Art Unit**	
	Justin T. Darrow	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *an amendment filed 11/19/2004*.

2. ☒ The allowed claim(s) is/are *1-24*.

3. ☒ The drawings filed on *23 January 2001* are accepted by the Examiner.

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
    a) ☐ All   b) ☐ Some*   c) ☐ None   of the:
        1. ☐ Certified copies of the priority documents have been received.
        2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
        3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the
            International Bureau (PCT Rule 17.2(a)).
    * Certified copies not received: _____ .

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
    (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
        1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____ .
    (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of
        Paper No./Mail Date _____ .
    Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)
1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material

5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____ .

DETAILED ACTION

1.   Claims 1-24 have been presented for examination. Claims 4, 7, 9, 11, 14, 17, 19, 21, 23, and 24 have been amended in an amendment filed 03/18/2004. Claims 1, 4, 6, 7, 11, 14, and 17 have been amended in an amendment filed 10/08/2004. Claims 1 and 4 have been amended in an amendment filed 11/19/2004. Claims 1-24 have been examined.

Allowable Subject Matter

2.   Claims 1-24 are allowed.

3.   The following is an examiner's statement of reasons for allowance:

Claims 1-3, 5, and 10; and 4 and 9 are drawn to methods for authenticating a first terminal to a second terminal. The closest prior art, Terao et al., U.S. Patent Application Publication No. US 2003/0097567 A1 in view of Hayashida, U.S. Patent No. 5,644,118 A describe similar methods. None of these inventors show or imply merging an obtained string with a user-entered, encrypted password to create an identification code. This particular step explicitly recited in independent claims 1 and 4 renders claims 1-3, 5, and 10; and 4 and 9, respectively, allowable.

Claims 4 and 9; and 14 and 19 are drawn to methods of authenticating a first terminal to a second terminal, respectively. The closest prior art, Stambler, U.S. Patent No. 5,793,302 A, discloses similar methods. However, Stambler neither shows nor motivates merging a string with a password using an applet at the first terminal, executing an encryption algorithm with a unique merging key. This composite step explicitly recited in intervening claims 4 and 14 renders claims 4 and 9; and 14 and 19, respectively, allowable.

Claim 6 is drawn to a method for authenticating a first terminal to a second terminal. The closest prior art, Terao et al., U.S. Patent Application Publication No. US 2003/0097567 A1 in view of Hayashida, U.S. Patent No. 5,644,118 A and further in view of Leith et al., U.S. Patent No. 5,196,840 A, disclose a similar method. Although Leith et al. embody adding randomness to different combinations of the PIN (see column 11, lines 15-41 and figure 9), none of these inventors neither teach nor suggest performing a block addition of a permutated string and permutated password. This distinct step incorporated into independent claim 6 renders claim 6 allowable.

Claims 7 and 8 are drawn to methods of authenticating a first terminal to a second terminal, respectively. The closest prior art, Terao et al., U.S. Patent Application Publication No. US 2003/0097567 A1 in view of Hayashida, U.S. Patent No. 5,644,118 A, discloses a similar method. However, none of these inventors depicts nor suggests obtaining the requested string by receiving a web page containing a program for generating requests and the string. This distinct step explicitly recited in independent claim 7 renders claims 7 and 8 allowable.

Claims 11-13, 15, 16, and 20; 14 and 19; and 17 and 18 are drawn to methods of authenticating a first terminal to a second terminal, respectively. The closest prior art, Terao et al., U.S. Patent Application Publication No. US 2003/0097567 A1, describe similar methods.

Terao et al. illustrate a method for authenticating a first terminal to a second terminal (see ¶¶ [0116]-[0118]; figure 4; authentication of a proof data generation device to a proof data verification device), comprising:

creating a string (see ¶ [0139]; figure 2, items 103 and 104; generating authentication data m) and storing it in association with an identification of a first terminal (see ¶¶ [0139]-

[0140]; figure 2, items 101, 103, and 104; storing the authentication data m in the access ticket

public key memory unit; see ¶¶ [0123]-[0125]; with the access ticket, t, in association with the

user unique identifying information, e);

sending the string to the first terminal (see ¶ [0140]; figure 4; sending the authentication

data m to the proof data generation device); and

receiving an identification code from the first terminal (see ¶ [0140]; figure 4; the proof

data generation device sending s to the proof data verification device) composed by merging the

sent string with a sender password (see ¶¶ [0148]-[0149]; figure 3, items 111, 112, 113, and 115;

a result from performing a calculation using the authentication data m and; see ¶¶ [0145]-[0146];

figure 3, items 111, 112, and 113; and an expression based on user unique identifying

information e; see ¶ [0123]; figure 3, item 112; where user unique identifying information e is

different for each user like a password).

Although Terao et al. describe calculating another value with received authentication

code (see ¶¶ [0153]-[0154]; figure 4; calculating an expression V from s) and comparing this

value with an expected value for authenticating the first terminal (see ¶ [0158]; figure 4;

verification is effected correctly when values V and V' coincide), they neither teach nor suggest

comparing the received identification code with an expected identification code. This particular

step explicitly recited in independent claims 11, 14, and 17 renders claims 11-13, 15, 16, and 20;

14 and 19; and 17 and 18, respectively, allowable.

Claims 21 and 22; 23; and 24 are drawn to authentication terminals, respectively. The

closest prior art, Terao et al., U.S. Patent Application Publication No. US 2003/0097567 A1,

describe similar authentication terminals.

Terao et al. depict an authentication terminal comprising:

a merge string library coupled to a processor to create a merge string and (see ¶ [0139];

figure 2, items 103 and 104; a random number generation unit generating authentication data m)

and to store it in association with an identification of a first terminal (see ¶¶ [0139]-[0140];

figure 2, items 101, 103, and 104; storing the authentication data m in the access ticket public

key memory unit; see ¶¶ [0123]-[0125]; with the access ticket, t, in association with the user

unique identifying information, e);

an output device to send the merge string to the second terminal (see ¶ [0140]; figure 4;

the authentication data memory unit sending the authentication data m to the proof data

generation device); and

an input device to receive an identification code from the second terminal (see ¶ [0140];

figure 4; the proof data generation device sending s to the authentication data memory unit of the

proof data verification device) being composed by merging the sent string with a second terminal

password (see ¶¶ [0148]-[0149]; figure 3, items 111, 112, 113, and 115; a result from performing

a calculation using the authentication data m and; see ¶¶ [0145]-[0146]; figure 3, items 111, 112,

and 113; and an expression based on user unique identifying information e; see ¶ [0123]; figure

3, item 112; where user unique identifying information e is different for each user like a

password).

Although Terao et al. describe a verification computation unit calculating another value

with received authentication code (see ¶¶ [0153]-[0154]; figure 4; calculating an expression V

from s) and comparing this value with an expected value for authenticating the second terminal

(see ¶ [0158]; figure 4; verification is effected correctly when values V and V' coincide), they

neither teach nor suggest an identification test library to compare the received identification code with an expected identification code. This distinct feature explicitly recited in independent claims 21, 23, and 24 renders claims 21 and 22; 23; and 24 allowable, respectively.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Telephone Inquiry Contacts

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Justin T. Darrow whose telephone number is (571) 272-3801, and whose electronic mail address is justin.darrow@uspto.gov. The examiner can normally be reached Monday-Friday from 8:30 AM to 5:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barrón, Jr., can be reached at (571) 272-3799.

The fax number for Formal or Official faxes to Technology Center 2100 is (703) 872-9306. In order for a formal paper transmitted by fax to be entered into the application file, the paper and/or fax cover sheet must be signed by a representative for the applicant. Faxed formal papers for application file entry, such as amendments adding claims, extensions of time, and statutory disclaimers for which fees must be charged before entry, must be transmitted with an authorization to charge a deposit account to cover such fees. It is also recommended that the cover sheet for the fax of a formal paper have printed "**OFFICIAL FAX**". Formal papers
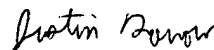
transmitted by fax usually require three business days for entry into the application file and

consideration by the examiner. Formal or Official faxes including amendments after final

rejection (37 CFR 1.116) should be submitted to (703) 872-9306 for expedited entry into the

application file. It is further recommended that the cover sheet for the fax containing an

amendment after final rejection have printed not only "**OFFICIAL FAX**" but also

"**AMENDMENT AFTER FINAL**".

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Any inquiry of a general nature or relating to the status of this application should be

directed to the Group receptionist whose telephone number is (571) 272-2100.

March 7, 2005

JUSTIN T. DARROW
PRIMARY EXAMINER
TECHNOLOGY CENTER 2100